

FILED IN CHAMBERS
U.S.D.C. Atlanta

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEB 10 2017
JAMES N. HATTEN, Clerk
By: *pjl* Deputy Clerk

UNITED STATES OF AMERICA

Criminal Indictment

v.

JAMES G. MALONEY

No. 1:16-cr-00237-AT-JSA

PROTECTIVE ORDER REGARDING CLASSIFIED INFORMATION

The parties have requested a Protective Order to prevent the unauthorized disclosure or dissemination of classified national security information and documents, which may be reviewed or made available to the Defendant and his counsel by the Government during the prosecution of this case. Pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. 3 (2006) ("CIPA"), the Security Procedures Established Pursuant to CIPA by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA section 9) and Rule 16(d) of the Federal Rules of Criminal Procedure, and the general supervisory authority of the Court, and in order to protect the national security, the following Protective Order is entered:

1. The Court finds that this case may involve information that has been classified in the interest of the national security. The storage, handling and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to which requires the appropriate security clearances. The purpose of this Order is to establish procedures that must be followed by counsel and the parties in this case. These procedures will apply to all pretrial, trial, post-trial and appellate matters concerning classified information and may be modified from time to time by further order of the Court acting under its inherent supervisory authority to ensure a fair and expeditious trial.
2. Definitions. The following definitions shall apply to this Order:
 - a. "Classified information" shall mean:
 - i. any document or information which has been classified by any executive agency in the interests of national security or pursuant to Executive Order 12958, as amended by Executive Order 13526, as "confidential," "secret," "top secret," or "sensitive compartmented information";
 - ii. any document or information now or formerly in the possession of a private party which (A) has been derived from information from

the United States Government that was classified, and (B) has been subsequently classified by the United States pursuant to Executive Order 12958, as amended by Executive Order 13526 as “confidential,” “secret,” “top secret,” or “sensitive compartmented information”;

- iii. verbal classified information known to the Defendant or defense counsel; or
 - iv. any information, regardless of place of origin and including “foreign Government information,” as that term is defined in Executive Order 12958, as amended by Executive Order 13526, that could reasonably be believed to contain classified information.
- b. “Document” shall mean any material containing information. The term “document” shall include, without limitation, written or printed matter of any kind, including originals, conforming copies, and non-conforming copies (e.g., a copy of an original with an added notation). The term “document” shall also include, without limitation, letters, reports, summaries, memoranda, notes, communications, telexes, cables, telecopies, telegrams, facsimiles, e-mails, microfilms, reports, photographs, charts, graphs, maps, invoices, accountings, worksheets,

bulletins, transcripts, and messages, as well as alterations, amendments, modifications, and changes of any kind to the foregoing; and all recordings of information on magnetic, electronic, or optical media (including but not limited to those on CD-ROM), typewriter ribbons, films and all manner of electronic data processing storage.

- c. "Access to classified information" means having access to, reviewing, reading, learning, or otherwise coming to know in any manner classified information.
 - d. "Secure area" means a sensitive compartmented information facility ("SCIF") accredited by a Classified Information Security Offices ("CISO") for the storage, handling, and control of classified information.
3. Information in the public domain is ordinarily not classified. However, if classified information is reported in the press or otherwise enters the public domain, the information does not lose its classified status merely because it is in the public domain. And information reported in the press or otherwise in the public domain may be considered classified and subject to the provisions of CIPA if the information, in fact, remains classified and is confirmed by any person who has, or has had, access to such classified information and that confirmation corroborates the information in question. Accordingly, any

attempt by the defense to have classified information that has been reported in the public domain confirmed or denied at trial or in any public proceeding in this case shall be governed by CIPA and all provisions of this Order.

4. All classified documents and information contained therein, shall remain classified unless the documents bear a clear indication that they have been declassified by the agency or department that originated the document or information contained therein (hereinafter, "originating agency").
5. In accordance with the provisions of CIPA and the Security Procedures promulgated by the Chief Justice of the United States pursuant to that Act, this court designates Carli V. Rodriguez-Feo as the Classified Information Security Officer and Debra M. Guerrero-Randall, Daniel O. Hartenstine, Matthew S. Juntz, Joan B. Kennedy, Shawn P. Mahoney, Maura L. Peterson, Winfield S. "Scooter" Slade and Harry J. Rucker, as alternate Classified Information Security Officers for this case for the purpose of providing security arrangements necessary to protect any classified information or documents that may be made available to the defense in connection with this case or that may be in the possession of the defense as a result of the Defendant's prior relationship with the Government. Defense counsel shall

seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information.

6. The Court has been advised that the United States Attorney John A. Horn and the Assistant United States Attorneys overseeing or assigned to this case, J. Russell Phillips and Stephen H. McClain, and Department of Justice attorneys, Richard R. Scott, Patrick T. Murphy, and Jennifer Kennedy Gellie have the requisite security clearances allowing them to have access to the classified documents and information that relate to this case. Any other Government attorneys who may in the future be designated to participate in the litigation of any part of this matter (or supervise such litigation) will have security clearances appropriate for the level of classification of any documents or information reviewed.
7. Upon receipt of appropriate security clearances, the Defendant's counsel, Craig A. Gillen and Anthony C. Lake, may have access to classified national security documents and information as required by the Government's discovery obligations and in accordance with the terms of this Protective Order, and any other orders pursuant to CIPA. It is expected that because of his work with various Government agencies, the Defendant, James G. Maloney, may also be given access to classified national security documents

and information to the extent required by Government discovery obligations and in accordance with the terms of this Protective Order, and any other orders pursuant to CIPA. Any additional person whose assistance the defense reasonably requires may only have access to classified information in this case after first obtaining from this Court, with prior notice to the Government, an approval for access to the required level of classification on a need-to-know basis, and after satisfying the other requirements described in this Order for access to classified information. The substitution, departure, or removal from this case of defense counsel or any other cleared person associated with the defense as an employee or witness or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

8. The CISO shall arrange for and maintain an appropriately approved secure area for the use of defense counsel. The CISO shall establish procedures to assure that the secure area is accessible to defense counsel during business hours and at other times upon reasonable request as approved by the CISO. The secure area shall contain a separate working area for defense counsel and will be outfitted with any secure office equipment requested by the defense that is reasonable and necessary to the preparation of the defense. The CISO,

in consultation with defense counsel, shall establish procedures to assure that the secure area may be maintained and operated in the most efficient manner consistent with the protection of classified information. No classified documents may be removed from the secure area unless so authorized by the CISO, with notice provided by the defense to the Court. The CISO shall not reveal to the Government the content of any conversations he or she may hear among the defense, nor reveal the nature of the documents being reviewed or the work being generated. The presence of the CISO shall not operate as a waiver, limit, or otherwise render inapplicable the attorney-client privilege. The parties further understand and agree that none of the procedures outlined in this Order shall be construed or operate as a waiver or limitation on attorney-client privilege or work product privilege.

9. Filing of Papers by the Defendant. Any pleading or other document filed by the Defendant shall be filed under seal with the Court through the CISO or her designee, unless the filing is a non-substantive pleading or document (e.g., motions for extensions of time, continuances, scheduling matters, etc.) not containing information that is or may be classified. Such non-substantive pleadings or documents may be filed on the public docket. Pleadings filed under seal with the CISO or her designee shall be marked, "Filed in Camera

and Under Seal with the Classified Information Security Officer or designee.”

The date and time of physical submission to the CISO or her designee shall be considered the date and time of filing. At the time of making a physical submission to the CISO or her designee, counsel shall file on the public record in the CM/ECF system a notice of filing that notifies the Court that a filing has been made. The notice should contain only the case caption and an unclassified title of the filing. The CISO or her designee shall immediately deliver, under seal, to the Court and counsel for the United States any pleading or document to be filed by the Defendant that may contain classified information. The CISO shall promptly examine the pleading or document and, in consultation with representatives of the appropriate agencies, determine whether the pleading or document contains classified information. If the CISO determines that the pleading or document contains classified information, he or she shall ensure that the portion of the document containing classified information, and only that portion, is marked with the appropriate classification marking and remains under seal. All portions of all paper filed by the Defendant that do not contain classified information will be placed in the public record.

10. Filing of Papers by the United States. Those portions of pleadings or documents filed by the United States that contain classified information shall be filed under seal with the court through the CISO or her designee. Such pleadings and documents shall be marked, "Filed in Camera and Under Seal with the Classified Information Security Officer or designee." The date and time of physical submission to the CISO or her designee shall be considered the date and time of filing. At the time of making a physical submission to the CISO or her designee, the Government shall file on the public record in the CM/ECF system a notice of filing that notifies the Court that a filing has been made. The notice should contain only the case caption and an unclassified title of the filing. The CISO or her designee shall immediately deliver, under seal, to the Court and counsel for the Defendant (unless such filing is an *ex parte* filing) any pleading or document to be filed by the Government that contains classified information.
11. The CISO shall maintain a separate sealed record for those materials which are classified. The CISO shall be responsible for maintaining the secured records for purposes of later proceedings or appeal.
12. Protection of Classified Information. The Court finds that in order to protect the classified information involved in this case, no individual other than

counsel for the United States, appropriately cleared Department of Justice employees, personnel of the originating agency, the Defendant, James G. Maloney and his counsel named above shall be allowed to obtain access to classified documents and information unless and until that person has been granted a security clearance by the Department of Justice through the CISO, and has obtained permission of the Court. No person except the Defendant and his counsel named above shall have access to the classified information involved in this case, unless and until that person, which includes any potential witnesses at trial, shall first have:

- e. received from the CISO the appropriate security clearance for the level of the classified information involved in this litigation; and
- f. signed the Memorandum of Understanding, in the form attached hereto, thereby agreeing to comply with the terms of this Order.

The signed Memorandum of Understanding shall be filed with the Court.

The substitution, departure, or removal for any reason from this case of counsel for the defense or anyone later cleared and associated with the defense as an employee or witness or otherwise shall not release that individual from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order. Before any person

other than counsel for the United States, appropriately cleared Department of Justice employees, and personnel of the originating agency, is permitted by the Court to inspect and review classified national security information, he or she must also sign the attached Memorandum of Understanding.

13. Access to Classified Information. The Defendant, his counsel, and any later cleared employees of counsel for the Defendant or cleared witnesses accompanied by counsel for the Defendant (hereinafter, "the defense") shall have access to classified information only as follows:

- a. All classified information produced by the Government to the defense in discovery or otherwise, and all classified information possessed, created or maintained by the defense, shall be stored, maintained and used only in the secure area established by the CISO. No classified information shall be maintained by the defense in any other place other than the secure area established by the CISO.
- b. The Defendant and his counsel shall have free access to the classified information made available to them in the secure area established by the CISO and shall be allowed to take notes and prepare documents with respect to those materials.

- c. No person, including counsel for the Defendant, shall copy or reproduce any classified information in any manner or form, except with the approval of the CISO or in accordance with the procedures established by the CISO for the operation of the secure area.
- d. All documents prepared by the defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information must be prepared in a secure area on word processing equipment approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits) containing classified information shall be maintained in the secure area unless and until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the United States.
- e. The defense shall discuss classified information only with other cleared persons and only in the secure area or in an area authorized by the CISO.
- f. The defense shall not disclose, without prior approval of the Court, the contents of any classified documents or information to any person not named in this Order except the Court, Court personnel, and the attorneys

for the United States identified by the CISO as having the appropriate clearances and the need to know. Counsel for the United States shall be given an opportunity to be heard in response to any defense request for disclosure to a person not named in this Order. Any person approved by the Court for disclosure under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to the Court the Memorandum of Understanding appended to the Order, and to comply with all the terms and conditions of the Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order, the Department of Justice shall promptly seek to obtain security clearances for them at the request of defense counsel.

- g. The defense, including the Defendant, counsel for the Defendant, and any other later cleared employees or defense witnesses, shall not discuss classified information over any standard commercial telephone instrument or office intercommunication systems, including but not limited to the internet, or in the presence of any person who has not been granted access by the Court to classified information.
- h. Any documents written by the defense that do or may contain classified information shall be transcribed, recorded, typed, duplicated, copied or

otherwise prepared only by persons who have received an appropriate approval for access to classified information, and must be created on equipment approved by the CISO as authorized to process classified information.

- i. If counsel for the Government advises Defendant's counsel that certain classified information or documents may not be disclosed to the Defendant, then defense counsel shall not disclose such information or documents to the Defendant without prior concurrence of counsel for the Government or, absent such concurrence, approval of the Court. Counsel for the Government shall be given an opportunity to be heard in response to any defense request for disclosure to the Defendant of such classified information.

14. Classified Information in Defendant's Possession. The Court has been advised by the Government that as a result of his prior Government contract work the Defendant may possess classified information. Accordingly, the Defendant is enjoined from disclosing any classified information to any unauthorized person during the pendency of this Protective Order. Nothing in this Protective Order shall be construed as a limitation on the Government in filing additional criminal charges against the Defendant in the event of an

unauthorized disclosure of classified information, or for the Court to enforce its Protective Order.

15. Classified Information Procedures Act. Procedures for the public disclosure of classified information by the defense shall be those established in sections 5 and 6 of CIPA. The Court may issue additional Protective Orders as needed.

16. Any unauthorized disclosure of classified information may constitute violations of United States criminal laws. In addition, any violation of the terms of this Order shall be brought immediately to the attention of this Court and may result in a charge of contempt of court and possible referral for criminal prosecution. Any breach of this Order may also result in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention, or negligent handling of classified documents or information could cause serious damage, and in some cases, exceptionally grave damage to the national security of the United States or may be used to the advantage of a foreign nation against the interests of the United States. This Protective Order is to ensure that those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to

receive it, without prior written authorization from the originating agency and in conformity with this Order.

17. All classified documents and information to which the defense (including the Defendant, counsel for the Defendant, any later cleared employee of counsel for the Defendant, or cleared defense witnesses) have access in this case are now and will remain the property of the United States. Upon demand of the CISO, these persons shall return to the CISO, all classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information. The notes, summaries and other documents prepared by the defense that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of the case. At the conclusion of this case, all such notes, summaries and other documents are to be destroyed by the CISO in the presence of defense counsel, if they choose to be present.
18. A copy of this Order shall be issued forthwith to the Defendant, defense counsel who shall be responsible for advising the Defendant, any co-counsel, employees of counsel for the Defendant, and defense witnesses who need to know of the contents of this Order. The Defendant, counsel for the Defendant, and any other individuals who will be provided access to the classified

information, shall execute the Memorandum of Understanding described in paragraph 12 of this Order, and counsel for the Defendant shall file executed originals of such documents with the Court and the CISO and serve an executed original upon the United States. The execution and filing of the Memorandum of Understanding is a condition precedent for the Defendant, counsel for the Defendant, or any other person assisting the defense to have access to classified information.

SO ORDERED, this 10th day of February 2017.



JUSTIN S. ANAND
UNITED STATES MAGISTRATE JUDGE

Requested and consented to by:

Counsel for the United States:

John A. Horn
United States Attorney
/s/ J. Russell Phillips
Assistant United States Attorney
Georgia Bar No. 576335
/s/ Stephen H. McClain
Assistant United States Attorney
Georgia Bar No. 143186
600 U.S. Courthouse
75 Ted Turner Drive SW
Atlanta, GA 30303

/s/ Jennifer Kennedy Gellie
Trial Attorney
New York Bar No. 4842852
/s/ Patrick T. Murphy
Trial Attorney
New York Bar No. 2750602
Counterintelligence and
Export Control Section
U.S. Department of Justice
600 E Street N.W.
Washington, D.C. 20004

Counsel for the Defendant:

Craig A. Gillen
Georgia Bar No. 294838
Anthony C. Lake
Georgia Bar No. 431149
Gillen Withers & Lake
3490 Piedmont Road, NE
One Securities Centre, Suite 1050
Atlanta, GA 30305